ELSEVIER

Linear Algebra and its Applications 298 (1999) 39–50

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

A matrix-decomposition theorem for $\mathrm{GL}_n(K)$

Florian Bünger, Klaus Nielsen *

Mathematisches Seminar, Universität Kiel, Ludewig-Meyn-Strasse 4, D-24098 Kiel, Germany

Received 27 November 1997; accepted 14 June 1999

Submitted by T.J. Laffey

Abstract

Given an arbitrary commutative field K, $n \in \mathbb{N}_{\geqslant 3}$ and two monic polynomials q and r over K of degree $n-1$ and n such that $q(0) \neq 0 \neq r(0)$. We prove that any non-scalar invertible $n \times n$ matrix M can be written as a product of two matrices A and B, where the minimum polynomial of A is divisible by q and B is cyclic with minimum polynomial r. This result yields that the Thompson conjecture is true for $\mathrm{PSL}_n(\mathbf{F}_3)$, $n \in \mathbb{N}_{\geqslant 3}$, and $\mathrm{PSL}_{2n+1}(\mathbf{F}_2)$, $n \in \mathbb{N}$. If G is such a group, then G has a conjugacy class Ω such that $G = \Omega^2$. In particular each element of G is a commutator.

Keywords: Matrix factorization; Product of cyclic matrices; Conjugacy class

1. Introduction

J.G. Thompson conjectured that every finite simple non-abelian group G possesses a conjugacy class Ω with $G = \Omega^2$. Lev [3] proves in his doctoral thesis that the Thompson conjecture is true for all finite simple projective linear groups $\mathrm{PSL}_n(\mathbf{F}_q)$ where $(n, q) \neq (2, 2), (2, 3)$. Lev [5] states the following theorem.

Theorem 1.1 (Lev). *Let K be a field, $n \in \mathbb{N}_{\geqslant 2}$, Ω_1, Ω_2 similarity classes of cyclic $n \times n$-matrices such that the minimum polynomial of Ω_1 decomposes in $K[x]$ into linear factors.*

(a) *If $n \geqslant 3$ and $|K| \geqslant 4$, then $\Omega_1\Omega_2$ contains every non-scalar matrix with determinant* $\det \Omega_1\Omega_2$.

* Corresponding author.

0024-3795/99/$ - see front matter
PII: S 0 0 2 4 - 3 7 9 5 (9 9) 0 0 1 3 8 - X

(b) *Let $n = 2$, then every non-scalar matrix with determinant* $\det \Omega_1\Omega_2$ *is contained in $\Omega_1\Omega_2$ if and only if the eigenvalues of Ω_1 are distinct or the minimum polynomial of Ω_2 also decomposes into $K[x]$ into linear factors.*

For $n = 2$ the proof follows by direct calculations. The arguments used in the proof for the case $n \geqslant 3$ are very interesting but rather complicated.

It follows from 1.1 that the Thompson-conjecture is true for $\mathrm{PSL}_n(K)$ provided that $|K| \geqslant 4$ and $n \geqslant 2$. For $n \geqslant 3$ our decomposition theorem yields the same result (cf. 6.1). We feel that its proof is less involved than the one of 1.1. Moreover, the Thompson-conjecture can be proved even for $\mathrm{PSL}_n(\mathbf{F}_3)$ where $n \geqslant 3$, and $\mathrm{PSL}_{2n+1}(\mathbf{F}_2)$ for all $n \in \mathbb{N}$ (cf. 6.1). Thus the only simple projective special linear groups for which our results do not imply the validity of the Thompson-conjecture are the groups $\mathrm{PSL}_{2n}(\mathbf{F}_2)$, $n \in \mathbb{N}_{\geqslant 2}$.

For general results concerning Thompson's conjecture in arbitrary finite simple Chevalley groups we refer to a paper of Ellers and Gordeev [1].

The main theorem of this paper is as follows.

Theorem 1.2. *Let K be a field and $n \in \mathbb{N}_{\geqslant 3}$. Suppose that $M \in \mathrm{GL}_n(K)$ is not a homothety, that Ω is a cyclic $\mathrm{GL}_n(K)$-similarity class and that $q \in K[x]$ is a monic polynomial of degree $n-1$ whose constant term $q(0)$ does not vanish. Then there is a $\mathrm{GL}_n(K)$-similarity class Δ whose minimum polynomial is divisible by q such that $M \in \Delta\Omega$.*

2. Notations

Throughout this paper let K be a (commutative) field. For a linear mapping π let $\mathrm{char}(\pi)$ denote the characteristic polynomial of π.

Notation 2.1. For $n \in \mathbb{N}$, we write I_n for the unit element in the group of all invertible $n \times n$-matrices over K. For $m \in \mathbb{N}_{\geqslant 2}$ the $m \times m$ permutation matrix corresponding to the cyclic permutation $(1 \ldots m)$ of the symmetric group on m letters is denoted by R (R_m). In matrix notation this reads

$$R = \begin{bmatrix} & I_{m-1} \\ 1 & \end{bmatrix} \in \mathrm{GL}_m(K).$$

Notation 2.2. For $n \in N$ let $J_n := (\delta_{i,n+1-j})_{1 \leqslant i,j \leqslant n-1} \in \mathrm{GL}_n(K)$. For $l, m \in \mathbb{N}$ and $A \in K^{l \times m}$ let $A^{\mathrm{r}} := J_l A J_m = (A_{l+1-i,m+1-j})_{(i,j) \in \mathbb{N}_{\leqslant l} \times \mathbb{N}_{\leqslant m}}$.

Remark 2.3. Let $l, m \in \mathbb{N}$ and $A \in K^{l \times m}$. The matrix A^{r} is obtained by reflection of A at the center of A. In particular, if $l = m$ and A is a lower triangular matrix, then A^{r} is an upper triangular matrix.

Notation 2.4. For $m \in \mathbb{N}$ and $A \in K^{m\times m}$ let

$$\begin{aligned} U_A &:= (A_{i,j})_{1\leqslant i,j\leqslant m-1},\\ u_A &:= (A_{1,m}, \ldots, A_{m-1,m})^{\mathrm{t}},\\ v_A &:= (A_{m,1}, \ldots, A_{m,m-1}),\\ L_A &:= (A_{i,j})_{2\leqslant i,j\leqslant m},\\ l_A &:= (A_{1,2}, \ldots, A_{1,m}). \end{aligned}$$

Moreover, put

$$Y_A := \operatorname{diag}(1, U_A) \in K^{m\times m} \text{ and } Z_A := \operatorname{diag}(L_A, 1) \in K^{m\times m}.$$

Remark 2.5. With the denotations of 2.4 we have

$$A = \begin{bmatrix} U_A & u_A \\ v_A & A_{m,m} \end{bmatrix} = \begin{bmatrix} A_{1,1} & l_A \\ * & L_A \end{bmatrix}.$$

If A is a regular triangular matrix then U_A, L_A, Y_A and Z_A are regular.

Observation 2.6. *Let $m \in \mathbb{N}$ and $A \in K^{m\times m}$. The following identities hold true*:
(i) $U_A^{\mathrm{t}} = U_{A^{\mathrm{t}}}$,
(ii) $U_A^{\mathrm{r}} = L_{A^{\mathrm{r}}}$,
(iii) $((Y_A)^{\mathrm{t}})^{\mathrm{r}} = Z_{(A^{\mathrm{t}})^{\mathrm{r}}}$.

Proof. (i) and (ii) are obvious since

$$A^{\mathrm{t}} = \begin{bmatrix} U_A & u_A \\ v_A & A_{m,m} \end{bmatrix}^{\mathrm{t}} = \begin{bmatrix} U_A^{\mathrm{t}} & v_A^{\mathrm{t}} \\ u_A^{\mathrm{t}} & A_{m,m} \end{bmatrix}$$

and

$$A^{\mathrm{r}} = \begin{bmatrix} U_A & u_A \\ v_A & A_{m,m} \end{bmatrix}^{\mathrm{r}} = \begin{bmatrix} A_{m,m} & v_A^{\mathrm{r}} \\ u_A^{\mathrm{r}} & U_A^{\mathrm{r}} \end{bmatrix}.$$

Finally, we see that

$$\begin{aligned} ((Y_A)^{\mathrm{t}})^{\mathrm{r}} &= (\operatorname{diag}(1, U_A)^{\mathrm{t}})^{\mathrm{r}} = \operatorname{diag}(1, U_{A^{\mathrm{t}}})^{\mathrm{r}} = \operatorname{diag}(U_{A^{\mathrm{t}}}^{\mathrm{r}}, 1)\\ &= \operatorname{diag}(L_{(A^{\mathrm{t}})}^{\mathrm{r}}, 1) = Z_{(A^{\mathrm{t}})^{\mathrm{r}}}. \qquad \square \end{aligned}$$

Notation 2.7. Let $r, s \in \mathbb{N}$, $m := r + s$, $a = (a_1, \ldots, a_{m-1}) \in K^{m-1}$ and $A \in K^{r-1\times s-1}$. We define

$$a^{\ulcorner} A := \left[\begin{array}{c|c} a_r & \ldots \quad a_{m-1} \\ \hline \vdots & \\ a_1 & \multicolumn{1}{c}{A} \end{array}\right] \in K^{r\times s}.$$

3. Special elements of cyclic conjugacy classes

Lemma 3.1. *Let $r \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_{r-1} \in K^*$, $\alpha_r \in K$. Suppose that $A \in K^{r\times r}$ is an upper triangular matrix with diagonal entries $A_{i,i} = \alpha_i$, $i \in \mathbb{N}_{\leqslant r}$. There is a unipotent upper triangular matrix $D \in \mathrm{GL}_r(K)$ such that*

$$Y_{D^{-1}} A D = \mathrm{diag}(\alpha_1, \ldots, \alpha_r).$$

Proof. We use induction on r. For $r = 1$ take $D := 1$. For $r \geqslant 2$ we can apply the induction hypothesis to $A' := U_A$. Observe that A' is regular since $\alpha_1, \ldots, \alpha_{r-1}$ are non-zero elements. Let $G \in \mathrm{GL}_{r-1}(K)$ be a unipotent upper triangular matrix satisfying

$$Y_{G^{-1}} A' G = \mathrm{diag}(\alpha_1, \ldots, \alpha_{r-1}).$$

Put

$$\begin{aligned} a &:= u_A, & H &:= U_{G^{-1}}, \\ h &:= u_{G^{-1}}, & h' &:= (0, h^{\mathrm{t}})^{\mathrm{t}}, \\ J &:= Y_{G^{-1}}, & g &:= -A'^{-1}a - \alpha_r (JA')^{-1} h' \end{aligned}$$

and

$$D := \begin{bmatrix} G & g \\ & 1 \end{bmatrix}.$$

We have $U_{D^{-1}} = G^{-1}$ and

$$Y_{D^{-1}} = \mathrm{diag}(1, G^{-1}) = \begin{bmatrix} 1 & & \\ & H & h \\ & & 1 \end{bmatrix} = \begin{bmatrix} J & h' \\ & 1 \end{bmatrix}.$$

Finally, we see:

$$\begin{aligned} Y_{D^{-1}} A D &= \begin{bmatrix} J & h' \\ & 1 \end{bmatrix} \begin{bmatrix} A' & a \\ & \alpha_r \end{bmatrix} \begin{bmatrix} G & g \\ & 1 \end{bmatrix} \\ &= \left[\begin{array}{c|c} JA' & Ja + \alpha_r h' \\ \hline & \alpha_r \end{array}\right] \begin{bmatrix} G & g \\ & 1 \end{bmatrix} \\ &= \left[\begin{array}{c|c} JA'G & JA'g + Ja + \alpha_r h' \\ \hline & \alpha_r \end{array}\right] \\ &= \mathrm{diag}(\alpha_1, \ldots, \alpha_r). \end{aligned}$$

This completes the proof. □

The following result is similar to Lemma 3.1.

Lemma 3.2. *Let $s \in \mathbb{N}$, $\beta_2, \ldots, \beta_s \in K^*$, $\beta_1 \in K$. Suppose that $B \in K^{s\times s}$ is an upper triangular matrix with diagonal entries $B_{i,i} = \beta_i$, $i \in \mathbb{N}_{\leqslant s}$. There is a unipotent upper triangular matrix $D \in \mathrm{GL}_s(K)$ such that*

$$DBZ_{D^{-1}} = \operatorname{diag}(\beta_1, \ldots, \beta_s).$$

Proof. We define $A := (B^{\mathrm{r}})^{\mathrm{t}}$. Then A is an upper $s \times s$ matrix with diagonal entries $A_{i,i} = \beta_{s+1-i}$, $i \in \mathbb{N}_{\leqslant s}$. Now 3.1 supplies a unipotent upper triangular matrix $G \in \mathrm{GL}_s(K)$ such that $Y_{G^{-1}} AG = \operatorname{diag}(\beta_s, \ldots, \beta_1)$. Consequently,

$$(G^{\mathrm{t}})^{\mathrm{r}} B((Y_{G^{-1}})^{\mathrm{t}})^{\mathrm{r}} = (\operatorname{diag}(\beta_s, \ldots, \beta_1)^{\mathrm{t}})^{\mathrm{r}} = \operatorname{diag}(\beta_1, \ldots, \beta_s).$$

Finally, $D := (G^{\mathrm{t}})^{\mathrm{r}}$ is a unipotent upper triangular matrix and $((Y_{G^{-1}})^{\mathrm{t}})^{\mathrm{r}} = Z_{D^{-1}}$ by 2.6. □

Now we put Lemmas 3.1 and 3.2 together.

Lemma 3.3. *Let $r, s \in \mathbb{N}, \alpha_1, \ldots, \alpha_{r-1}, \beta_2, \ldots, \beta_s \in K^*$ and $\alpha_r, \beta_1 \in K$. Suppose that $A \in K^{r\times r}$ and $B \in K^{s\times s}$ are upper triangular matrices with diagonal entries $A_{i,i} = \alpha_i$, $i \in \mathbb{N}_{\leqslant r}$, and $B_{i,i} = \beta_i$, $i \in \mathbb{N}_{\leqslant s}$ and C is an arbitrary $r \times s$ matrix. Then*

$$\begin{bmatrix} 1 & \\ & D^{-1} \end{bmatrix} \begin{bmatrix} A & C' \\ & B \end{bmatrix} \begin{bmatrix} D & \\ & 1 \end{bmatrix} = \left[\begin{array}{c|c} \operatorname{diag}(\alpha_1, \ldots, \alpha_r) & C \\ \hline & \operatorname{diag}(\beta_1, \ldots, \beta_s) \end{array}\right]$$

for some unipotent upper triangular matrix $D \in \mathrm{GL}_{r+s-1}(K)$ and a matrix $C' \in K^{r\times s}$.

Proof. By Lemmas 3.1 and 3.2 there are unipotent upper triangular matrices $P \in \mathrm{GL}_r(K)$ and$Q \in \mathrm{GL}_s(K)$ such that

$$Y_{P^{-1}} AP = \operatorname{diag}(\alpha_1, \ldots, \alpha_r) \text{ and } QBZ_{Q^{-1}} = \operatorname{diag}(\beta_1, \ldots, \beta_s).$$

Let $v = (\delta_{i,r})_{1\leqslant i\leqslant r} \in K^r$ denote the row with the first $r-1$ entries 0 and the last entry equals 1.

Put

$$\begin{array}{lll} E := U_{P^{-1}}, & e := u_{P^{-1}}, & e' := (0, e^{\mathrm{t}})^{\mathrm{t}}, \\ F := L_{Q^{-1}}, & f := (h, 0), & f' := (f, 0), \\ g := l_Q, & g' := (1, g), & \\ Y := Y_{D^{-1}}, & Z := Z_{Q^{-1}}, & C' := Y^{-1}(C - YAv^{\mathrm{t}} f' - e'g'BZ)Z^{-1} \end{array}$$

and

$$D := \begin{bmatrix} P & v^{\mathrm{t}} f \\ & F \end{bmatrix}.$$

First we observe:

$$\begin{bmatrix} D & \\ & 1 \end{bmatrix} = \begin{bmatrix} P & v^{\mathrm{t}} f' \\ & Z \end{bmatrix} \quad \text{and} \quad Q = \begin{bmatrix} 1 & f \\ & F \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -fF^{-1} \\ & F^{-1} \end{bmatrix},$$

i.e., $g = -fF^{-1}$. Since $P^{-1}v^{\mathrm{t}} = (e^{\mathrm{t}}, 1)$ we get

$$P^{-1}v^{\mathrm{t}}g = \left[\begin{array}{c} eg \\ \hline g \end{array}\right].$$

This yields

$$D^{-1} = \left[\begin{array}{cc} P^{-1} & -P^{-1}v^{\mathrm{t}}fF^{-1} \\ & F^{-1} \end{array}\right] = \left[\begin{array}{c|c} P^{-1} & \begin{array}{c} eg \\ \hline g \end{array} \\ \hline & F^{-1} \end{array}\right].$$

Thus we deduce

$$\left[\begin{array}{cc} 1 & \\ & D^{-1} \end{array}\right] = \left[\begin{array}{c|c|c} 1 & & \\ \hline & P^{-1} & \begin{array}{c} eg \\ \hline g \end{array} \\ \hline & & F^{-1} \end{array}\right] = \left[\begin{array}{c|c|c|c} 1 & & & \\ \hline & E & e & eg \\ \hline & & 1 & g \\ \hline & & & F^{-1} \end{array}\right] = \left[\begin{array}{c|c} Y & e'g' \\ \hline & Q \end{array}\right]$$

and

$$\begin{aligned} \left[\begin{array}{cc} 1 & \\ & D^{-1} \end{array}\right]\left[\begin{array}{cc} A & C' \\ & B \end{array}\right]\left[\begin{array}{cc} D & \\ & 1 \end{array}\right] &= \left[\begin{array}{cc} Y & e'g' \\ & Q \end{array}\right]\left[\begin{array}{cc} A & C' \\ & B \end{array}\right]\left[\begin{array}{cc} P & v^{\mathrm{t}}f' \\ & Z \end{array}\right] \\ &= \left[\begin{array}{cc} YA & YC' + e'g'B \\ & QB \end{array}\right] \\ &= \left[\begin{array}{c|c} YAP & YAv^{\mathrm{t}}f' + YC'Z + e'g'BZ \\ \hline & QBZ \end{array}\right] \\ &= \left[\begin{array}{c|c} \mathrm{diag}(\alpha_1, \ldots, \alpha_r) & C \\ \hline & \mathrm{diag}(\beta_1, \ldots, \beta_s) \end{array}\right]. \qquad \square \end{aligned}$$

A reformulation of Lemma 3.3 is as follows.

Lemma 3.4. *Under the assumptions of Lemma* 3.3 *there is a unipotent upper triangular matrix* $G \in \mathrm{GL}_{r+s}(K)$ *and a matrix* $C' \in K^{r\times s}$ *such that*

$$G^{-1}R\left[\begin{array}{cc} A & C' \\ & B \end{array}\right]G = R\left[\begin{array}{c|c} \mathrm{diag}(\alpha_1, \ldots, \alpha_r) & C \\ \hline & \mathrm{diag}(\beta_1, \ldots, \beta_s) \end{array}\right].$$

Proof. Choose D and C' as in the conclusion of 3.3 and put $G := \mathrm{diag}(D, 1)$. Since $R^{-1}G^{-1}R = \mathrm{diag}(1, D^{-1})$ Lemma 3.3 yields the assertion. $\square$

Lemma 3.5. *Let* $n \in \mathbb{N}_{\geqslant 2}$, $r \in \mathbb{N}_{\leqslant n-1}$, $\alpha_1, \ldots, \alpha_{r-1}, \alpha_{r+1}, \ldots, \alpha_n \in K^*$, $\alpha_r \in K$ *and* $c \in K^{n-1}$. *The matrix*

$$M := R\left[\begin{array}{c|c} \mathrm{diag}(\alpha_1, \ldots, \alpha_r) & c^{\ulcorner}0 \\ \hline & \mathrm{diag}(\alpha_{r+1}, \ldots, \alpha_n) \end{array}\right]$$

is cyclic and its characteristic polynomial is

$$x^n - \sum_{t=r}^{n-1} c_t \left(\prod_{u=t+2}^{n} \alpha_u \right) x^t - \left(\alpha_1 \prod_{u=r+2}^{n} \alpha_u \right) \sum_{t=1}^{r-1} \left(\prod_{u=2}^{r-t} \alpha_u \right) c_t x^t - \prod_{i=1}^{n} \alpha_i .$$

In particular, if $p \in K[x]$ *is a monic polynomial of degree n and* $p(0) = -\alpha_1 \cdots \alpha_n$, *then c can be chosen such that* $\operatorname{char}(M) = p$.

Proof. For $i \in \mathbb{N}$ let $e_i = (\delta_{i,j})_{j \in \mathbb{N}_{\leqslant n}}$ denote the row of length n whose ith entry is 1 and whose other entries are zero. Put $D := R^{-1}M$, $s := n - r$, $v := e_r$ and $v^i := vM^i$, $0 \leqslant i \leqslant n$. We claim that $\{v^i; 0 \leqslant i \leqslant n-1\}$ is a basis for K^n. Precisely, we will compute the M-annihilator of v.

Step 1. For $i \in \{0, \ldots, s\}$ we have

$$v^i = \left(\prod_{j=1}^{i} \alpha_{r+j} \right) e_{r+i} . \tag{3.1}$$

Proof. This formula is verified by a trivial induction on i. For $i = 0$ the identity $v^i = v^0 = v = e_r$ proves (3.1).

Now suppose that $i \in \mathbb{N}_{\leqslant s}$ and that (3.1) is true for $i-1$. Since $r+i-1 \leqslant n-1$, we have

$$e_{r+i-1}M = e_{r+i-1}RD = e_{r+i}D = \alpha_{r+i}e_{r+i} .$$

Now the induction hypothesis yields

$$v^i = v^{i-1}M = \left(\prod_{j=1}^{i-1} \alpha_{r+j} \right) e_{r+i-1}M = \prod_{j=1}^{i} \alpha_{r+j} e_{r+i} . \qquad \square$$

Observe that $\alpha_{r+1} \neq 0$.

Step 2. For $i \in \{1, \ldots, r-1\}$ we have

$$\begin{aligned} e_1 M^i &= \left(\prod_{j=2}^{i+1} \alpha_j \right) e_{i+1} + \sum_{j=1}^{i} \left(\prod_{l=2}^{j} \alpha_l \right) c_{r-j} e_{r+1} M^{i-j} \\ &= \left(\prod_{j=2}^{i+1} \alpha_j \right) e_{i+1} + \alpha_{r+1}^{-1} \sum_{j=1}^{i} \left(\prod_{l=2}^{j} \alpha_l \right) c_{r-j} v^{i-j+1} . \end{aligned} \tag{3.2}$$

Proof. The assertion is trivial for $r = 1$. Thus we may assume that $r \geqslant 2$.

We use induction on i. First observe that (3.1) yields $e_{r+1} = \alpha_{r+1}^{-1} v^1$. If $i = 1$, then

$$e_1 M = e_1 RD = e_2 D = \alpha_2 e_2 + c_{r-1} e_{r+1} = \alpha_2 e_2 + \alpha_{r+1}^{-1} c_{r-1} v^1 .$$

Now suppose that $r \geqslant 3$, $i \in \{2, \dots, r-1\}$ and that (3.2) holds true for $i-1$. Then $e_i M = e_i RD = e_{i+1} D = \alpha_{i+1} e_{i+1} + c_{r-i} e_{r+1}$. The induction hypothesis yields

$$\begin{aligned} e_1 M^i = (e_1 M^{i-1}) M &= \left(\prod_{j=2}^{i} \alpha_j \right) e_i M + \sum_{j=1}^{i-1} \left(\prod_{l=2}^{j} \alpha_l \right) c_{r-j} e_{r+1} M^{i-j} \\ &= \left(\prod_{j=2}^{i+1} \alpha_j \right) e_{i+1} + \sum_{j=1}^{i} \left(\prod_{l=2}^{j} \alpha_l \right) c_{r-j} e_{r+1} M^{i-j} \\ &= \left(\prod_{j=2}^{i+1} \alpha_j \right) e_{i+1} + \alpha_{r+1}^{-1} \sum_{j=1}^{i} \left(\prod_{l=2}^{j} \alpha_l \right) c_{r-j} v^{i-j+1}. \end{aligned}$$ □

For $i \in \{0, \dots, s\}$ and $j \in \{0, \dots, r-1\}$ put

$$\beta_i := \prod_{k=1}^{i} \alpha_{r+k} \quad \text{and} \quad \gamma_j := \prod_{k=2}^{j+1} \alpha_k.$$

Let $i \in \mathbb{N}_{\leqslant r}$. Then (3.1) and (3.2) yield

$$\begin{aligned} v^{s+i} = v^s M^i &= \beta_s (e_n RD) M^{i-1} = \beta_s e_1 D M^{i-1} \\ &= \beta_s \left(\alpha_1 e_1 + \sum_{j=r+1}^{n} c_{j-1} e_j \right) M^{i-1} \qquad (3.3) \\ &= \beta_s \left(\alpha_1 \gamma_{i-1} e_i + \alpha_1 \alpha_{r+1}^{-1} \sum_{j=1}^{i-1} \gamma_{j-1} c_{r-j} v^{i-j} + \sum_{j=r+1}^{n} c_{j-1} \beta_{j-r}^{-1} v^{j-r+i-1} \right). \end{aligned}$$

Since $\beta_i \neq 0$ for $i \in \{0, \dots, s\}$ step 1 implies $\langle e_r, \dots, e_n \rangle = \langle v^0, \dots, v^s \rangle$. Since $\gamma_i \neq 0$ for $i \in \{0, \dots, r-2\}$ (3.3) implies $e_i \in \langle v^0, \dots, v^{n-1} \rangle$ for $i \in \mathbb{N}_{\leqslant r-1}$. Thus M is cyclic. For $i = r$ (3.3) reads

$$v^n = \beta_s \left(\alpha_1 \gamma_{r-1} v^0 + \alpha_1 \alpha_{r+1}^{-1} \sum_{j=1}^{r-1} \gamma_{j-1} c_{r-j} v^{r-j} + \sum_{j=r+1}^{n} c_{j-1} \beta_{j-r}^{-1} v^{j-1} \right).$$

As $\beta_s \alpha_1 \gamma_{r-1} = \alpha_1 \cdots \alpha_n$ this means that

$$x^n - \sum_{t=r}^{n-1} c_t \beta_s \beta_{t-r+1}^{-1} x^t - \sum_{t=1}^{r-1} c_t \beta_s \alpha_1 \alpha_{r+1}^{-1} \gamma_{r-t-1} x^t - \prod_{i=1}^{n} \alpha_i$$

$$= x^n - \sum_{t=r}^{n-1} c_t \left(\prod_{u=t+2}^{n} \alpha_u \right) x^t - \left(\alpha_1 \prod_{u=r+2}^{n} \alpha_u \right) \sum_{t=1}^{r-1} \left(\prod_{u=2}^{r-t} \alpha_u \right) c_t x^t - \prod_{i=1}^{n} \alpha_i$$

is the M-annihilator of v. □

4. Products of two cyclic conjugacy classes

In this section we want to prove an analogue to Lev's result [4], Lemma 5, that applies also to singular matrices. The arguments require a generalized version of Sourour's Theorem 1 in [6]. The proof of this generalization is the same as the proof of Theorem 4.5.4, p. 289, given in [2] together with the second subsequent exercise. The assumption $K = \mathbb{C}$ of the proof given in [2] is not used. (Compare also [7, Theorem 1].)

Theorem 4.1 (Sourour). *Let $A \in K^{n\times n}$, $k := \operatorname{rank} A$, $\beta_1, \ldots, \beta_n, \gamma_1, \ldots, \gamma_k \in K^*$ and $\gamma_{k+1} = \cdots = \gamma_n = 0$. If A is regular, assume that A is not a homothety and that $\prod_{j=1}^{n} \beta_j \gamma_j = \det A$. There exist a lower triangular matrix B, an upper triangular matrix C such that $B_{i,i} = \beta_i$, $C_{i,i} = \gamma_i$ for $i \in \mathbb{N}_{\leqslant n}$ and A is similar to BC.* □

Theorem 4.2. *Let $n \in \mathbb{N}_{\geqslant 2}$, $M \in K^{n\times n}$, Δ a cyclic similarity class in $\mathrm{GL}_n(K)$ and Ω a cyclic similarity class in $K^{n\times n}$ with the following properties*:

(i) $\operatorname{char}(M) = pp'$ *for monic polynomials* $p, p' \in K[x]$, $p'(0) \neq 0$ *such that p is prime to p'*;
(ii) $\dim \ker M = \dim \ker \Omega \leqslant 1$;
(iii) $\det M = \det \Delta \det \Omega$.

Then $M \in \Delta\Omega$.

Proof. Let $s := \deg(p) \in \mathbb{N}$ and $t := \deg(p') \in \mathbb{N}$. Then $s + t = n$ and we may assume that $M = \operatorname{diag}(A, A')$ for some $A \in K^{s\times s}$ and some $A' \in \mathrm{GL}_t(K)$ such that $\operatorname{char}(A) = p$ and $\operatorname{char}(A') = p'$. By Sourour's Theorem 4.1 or using a trivial argument [in the scalar case] we can find elements $\gamma_1, \ldots, \gamma_{s-1}, \gamma'_1, \ldots, \gamma'_{t-1} \in K^*$, $\gamma_s = (\gamma_1 \cdots \gamma_{s-1})^{-1} \det A$, $\gamma'_t = (\gamma'_1 \cdots \gamma'_{t-1}) \det \Delta^{-1} \det A'$ and matrices

$$B = \begin{bmatrix} 1 & & \\ & \ddots & \\ * & & 1 \end{bmatrix} \in \mathrm{GL}_s(K), \quad C = \begin{bmatrix} \gamma_1 & & * \\ & \ddots & \\ & & \gamma_s \end{bmatrix} \in K^{s\times s},$$

$$B' = \begin{bmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ * & & & \det \Delta \end{bmatrix} \in \mathrm{GL}_t(K), \quad C' = \begin{bmatrix} \gamma'_1 & & * \\ & \ddots & \\ & & \gamma'_t \end{bmatrix} \in \mathrm{GL}_t(K),$$

such that A is similar to BC and A' is similar to $B'C'$. Thus we may assume that $M = \operatorname{diag}(BC, B'C')$. We have $\det B \det B' = \det \Delta$ and

$$\det C \det C' = \det A \det \Delta^{-1} \det A' = \det M \det \Delta^{-1} = \det \Omega.$$

Now Lemmas 3.3 and 3.5 supply $P, Q \in K^{s\times t}$ such that

$$Y := R\begin{bmatrix} B^{\mathrm{r}} & P \\ & B'^{\mathrm{r}} \end{bmatrix} \in \Delta \quad \text{and} \quad Z := R\begin{bmatrix} C & Q \\ & C' \end{bmatrix} \in \Omega.$$

Put $J := \operatorname{diag}(J_s, J_t)$. A simple computation shows that $R^J = R^{\mathrm{r}} = R^{\mathrm{t}} = R^{-1}$. Finally, we get

$$Y^{RJ}Z = \begin{bmatrix} B & P^{\mathrm{r}} \\ & B' \end{bmatrix} R^{-1} R \begin{bmatrix} C & Q \\ & C' \end{bmatrix} = \begin{bmatrix} A & * \\ & A' \end{bmatrix}.$$

Since $\operatorname{char}(A)$ is prime to $\operatorname{char}(A')$ the matrix occuring on the right-hand side of the last equation is similar to M. The proof is completed as $Y^{RJ}Z$ belongs to $\Delta\Omega$. □

Observe that condition (iv) of Theorem 4.2 is always true when M and A are singular.

5. Proof of the main theorem

Case A: M is not cyclic. Since M is not a homothety we may assume that $M = \operatorname{diag}(M_1, M_2)$ where

$$M_2 = \begin{bmatrix} 0 & I_{m-1} \\ \delta & p \end{bmatrix} \in \mathrm{GL}_m(K), \quad p \in K^{m-1},$$

is a companion matrix for some $m \in \mathbb{N}_{\geqslant 2}$. Write

$$M = \begin{bmatrix} N & a \\ b & \gamma \end{bmatrix},$$

where $N := U_M, a := u_M, b := v_M$ (cf. 2.4), $\gamma := M_{n,n}$. Then N is singular, $\dim \ker N = 1$ and $\operatorname{char}(N) = \operatorname{char}(M_1)x^{m-1}$. Since $m \geqslant 2$, $\operatorname{char}(M_1)$ and x^{m-1} are prime to each other we may assume by Theorem 4.2 that $N = CD$ where $C \in \mathrm{GL}_{n-1}(K)$ has minimum polynomial q and $D \in K^{n-1\times n-1}$ is a cyclic nilpotent upper triangular matrix. Let $d := C^{-1}a$. Since

$$\begin{bmatrix} C^{-1} & \\ & 1 \end{bmatrix}\begin{bmatrix} CD & a \\ b & \gamma \end{bmatrix} = \begin{bmatrix} D & d \\ b & \gamma \end{bmatrix}$$

is regular and the last row of D is zero, we see that $d_{n-1} \neq 0$. By Lemmas 3.3 and 3.5 we find $e \in K^{n-1}$ and $\beta \in K^*$ such that

$$E := \begin{bmatrix} D & d \\ e & \beta \end{bmatrix} \in \Omega. \tag{5.1}$$

Put

$$A := ME^{-1} = \begin{bmatrix} F & g \\ h & \alpha \end{bmatrix}, \quad F := U_A, \quad g := u_A, \quad h := v_A, \quad \alpha := A_{n,n}.$$

Then we have

$$\begin{bmatrix} CD & a \\ b & \gamma \end{bmatrix} = M = AE = \begin{bmatrix} FD + ge & Fd + \beta g \\ hD + \alpha e & hd + \alpha\beta \end{bmatrix}.$$

This implies $CD = FD + ge$. Since the first column of D is zero, we get $ge_1 = 0$ and $e_1 \neq 0$ (cf. 5.1). This means that $g = 0$ and $C[D|d] = [CD|a] = F[D|d]$. But $[D|d]$ has rank $n-1$, hence $F = C$ and case A is finished.

Case B: M is cyclic. Let $\alpha := (-1)^{n-1} q(0) \det M \det \Omega^{-1}$.

B1: $q \neq (x-\alpha)^{n-1}$. Choose an arbitrary matrix $A \in \mathrm{GL}_n(K)$ whose minimum polynomial is divisible by q and $x - \alpha$. The assumption yields that $\mathrm{char}(A)$ has two distinct prime divisors. Hence Theorem 4.2 proves $A \in M^{\mathrm{GL}_n(K)}\Omega^{-1}$ and we are done.

B2: $q = (x-\alpha)^{n-1}$. Since M is cyclic, we may assume that

$$M = \begin{bmatrix} 0 & I_{n-1} \\ b & \gamma \end{bmatrix}$$

is a companion matrix. Put $N := U_M, a := u_M, b := v_M$ (cf. 2.4) and $\gamma := M_{n,n}$. Then N is a cyclic nilpotent upper triangular matrix. Let $C \in \mathrm{GL}_{n-1}(K)$ be a cyclic upper triangular matrix with diagonal entries $C_{i,i} = \alpha$, $i \in \mathbb{N}_{\leqslant n-1}$. Then $D := C^{-1}N$ is a cyclic nilpotent upper triangular matrix. Now we can proceed as in case A. This completes the proof. □

6. The Thompson conjecture for $\mathrm{PSL}_n(K)$

As we said in the introduction, we can use Theorem 1.2 in order to prove the Thompson-conjecture for $\mathrm{PSL}_n(K)$ if $|K| \geqslant 3$ and $\mathrm{PSL}_{2n+1}(\mathbf{F}_2)$, $n \in \mathbb{N}$.

Theorem 6.1. *Let K be a field and $n \in \mathbb{N}_{\geqslant 2}$. If $|K| \leqslant 3$, we assume that $n \geqslant 3$. Moreover, if $K = \mathbf{F}_2$, we assume that n is odd. Then $\mathrm{PSL}_n(K)$ contains a conjugacy class Ω such that $\mathrm{PSL}_n(K) = \Omega^2$.*

Proof. In the sequel we tacitly use the fact that a $\mathrm{GL}_n(K)$-conjugacy class contained in $\mathrm{SL}_n(K)$ which possesses an eigenvalue of multiplicity one is a $\mathrm{SL}_n(K)$-conjugacy class.

Case A: $|K| \geqslant 4$. Choose $\alpha \in K \setminus \{0, 1, -1\}$. Let $q := (x-1)^{n-2}(x - \alpha^{-1})$ and Ω be the cyclic $\mathrm{GL}_n(K)$-conjugacy class with characteristic polynomial $(x-\alpha)q$. This polynomial is selfreciprocal. Hence $\Omega = \Omega^{-1}$ thus $1 \in \Omega^2$. We have $\det \Omega = 1$ and α is an eigenvalue of Ω of multiplicity one. Hence Ω is a $\mathrm{SL}_n(K)$-conjugacy class. Let $M \in \mathrm{SL}_n(K)$, M not a homothety. Then $x - (-1)^{n-1} q(0) \det M \det \Omega^{-1}$

$= x - \alpha$ is prime to q. If $n \geqslant 3$, then 1.2 supplies $A \in \mathrm{GL}_n(K)$ with minimum polynomial $(x-\alpha)q$ and $B \in \Omega$ such that $M = AB$. As $A \in \Omega$, hence $M \in \Omega^2$. If $n = 2$, then $\mathrm{char}(\Omega) = (x-\alpha)(x-\alpha^{-1})$ and M is contained in Ω^2 by the simple part of Lev's Theorem 1.1.

Case B: $|K| \leqslant 3$. Then $n \geqslant 3$ by our assumption.

B1: n is odd. Then $n-1 \geqslant 2$ is even. For $K = \mathbf{F}_2$ let $q := (x^2+x+1)^{(n-1)/2}$ and if $K = \mathbf{F}_3$ put $q := (x^2+1)^{(n-1)/2}$. Then q is a monic selfreciprocal polynomial and $q(0) = 1$. Let Ω be the cyclic $\mathrm{GL}_n(K)$-conjugacy class with characteristic polynomial $(x-1)q$. It is easy to see that $\det \Omega = 1$, $\Omega = \Omega^{-1}$ and that Ω is a $\mathrm{SL}_n(K)$-conjugacy class. If $M \in \mathrm{SL}_n(K)$ is not a homothety then $x - (-1)^{n-1}q(0)\det M$ $\det \Omega^{-1} = x - (-1)^{n-1} = x - 1$ is prime to q. Again 1.2 yields $M \in \Omega^2$.

B2: n is even. Then $K = \mathbf{F}_3$, $n \geqslant 4$ and $-1 \in \mathrm{SL}_n(K)$. Put

$$q := (x+1)(x^2+x-1)(x^2+1)^{(n-4)/2}.$$

Let Ω be the cyclic $\mathrm{GL}_n(K)$-conjugacy class with characteristic polynomial $(x-1)q$. Then $\det \Omega = (-1)^n \mathrm{char}(\Omega)(0) = (-1)^{n+2} = 1$ and Ω is a $\mathrm{SL}_n(K)$-conjugacy class as Ω possesses eigenvalues of multiplicity one. Furthermore $\Omega = -\Omega^{-1}$ implies $-1 \in \Omega^2$. If $M \in \mathrm{SL}_n(K)$ is not a homothety then $x - (-1)^{n-1}q(0)$ $\det M \det\ \Omega^{-1} = x - (-1)^{n-2} = x - 1$ is prime to q and 1.2 yields $M \in \Omega^2$. The proof is completed. □

References

[1] E.W. Ellers, N. Gordeev, On the conjectures of J. Thompson and O. Ore, Trans. Amer. Math. Soc. 350 (1998) 3657–3671.
[2] R. Horn, C. Johnson, Topics in Matrix Analysis, Cambridge University Press, Cambridge, 1991.
[3] A. Lev, Products of Conjugacy Classes in the Groups $\mathrm{PSL}_n(F)$, Ph.D. Thesis, Tel-Aviv University, 1994.
[4] A. Lev, Products of cyclic conjugacy classes in the groups $\mathrm{PSL}(n, F)$, Linear Algebra Appl. 179 (1993) 59–83.
[5] A. Lev, Products of cyclic similarity classes in the groups $\mathrm{GL}_n(F)$, Linear Algebra Appl. 202 (1994) 235–266.
[6] A.R. Sourour, A factorization theorem for matrices, Linear and Multilinear Algebra 19 (1986) 141–147.
[7] A.R. Sourour, K. Tang, Factorization of singular matrices, Proceedings of the American Mathematical Society 116 (3) (1992) 629–634.